IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH JACESTOREY4@ICLOUD.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	Case No. 6:20MJ00020 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Task Force Officer Daniel Bailey, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Task Force Officer with the Drug Enforcement Administration (DEA) and have been since 2017. I am also a Detective with the Lynchburg Police Department (Virginia) and be been so employed since 2002. I am currently assigned to investigate drug trafficking organizations as a member of the DEA, Washington Field Division/Roanoke Resident Office. My duties as a Task Force Officer involve the investigation of various criminal activities of narcotics traffickers and their associates. In investigating these matters, I have acted as a case agent, an undercover agent, and a contact agent for confidential sources. These investigations

have resulted in the issuance of federal search warrants, seizure warrants, indictments, and convictions of persons for federal narcotics violations. During my employment as a law enforcement officer, I have received multiple hours of training in narcotics enforcement and investigative techniques, and I have personally participated in numerous investigations. I have also spoken on numerous occasions with informants, suspects, and other experienced narcotics traffickers concerning the methods and practices of drug traffickers, including the methods and practices used by traffickers of methamphetamine, heroin, and cocaine. I have been involved in the execution of numerous search warrants on electronic devices, including cellphones, and in obtaining location information for those devices.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations of 21 U.S.C. §§ 841, 843, and 846, as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The United States, including the DEA and the Lynchburg Police Department, is conducting a criminal investigation of Jermel STOREY ("STOREY") and others regarding violations of distribution and possession with intent to distribute cocaine in violation of 21 U.S.C. § 841(a)(1) and conspiracy to distribute cocaine and marijuana in violation of 21 U.S.C. § 846.

7. Multiple sources of information indicate that, prior to approximately 2013, STOREY lived in the Lynchburg, VA area and was a distributor of controlled substances. STOREY then relocated to Charlotte, NC, located within the Western District of North Carolina, but continued to supply narcotics distributors in the Lynchburg, VA area, located within the Western District of Virginia.

8. Multiple sources of information indicate that STOREY uses various cell phones to communicate about and facilitate drug transactions.

9. In December 2018, the LPD executed a Virginia-issued search warrant on a cellular phone belonging to Timothy PAIGE. Upon analysis of the data extracted from that cellular phone, this applicant determined that PAIGE was communicating, via text messaging, with a phone number identified as being used by STOREY during that time. The phone number, used by STOREY, sent PAIGE photographs of brick shaped items wrapped in plastic wrap. This applicant, knows through his training and experience that those bricks were consistent with kilogram bricks of cocaine. This applicant also observed text messages exchanged between STOREY and PAIGE negotiating cocaine purchases. These communications occurred between October 19, 2018 and November 25, 2018.

10. In January 2019, a law enforcement officer conducted an interview with Source of Information #1 ("SOI-1") who had been arrested for drug trafficking in New Haven, CT. SOI-1 advised law enforcement that STOREY was SOI-1's source of supply for kilogram quantities of cocaine. SOI-1 advised that SOI-1 would communicate with STOREY via cellular phone to arrange for deliveries of narcotics.

11. In July 2019, this applicant conducted an interview with Source of Information #2 ("SOI-2") who had been arrested in February of 2019 for Distribution of Cocaine hydrochloride in Lynchburg, VA, which is in the Western District of Virginia. SOI-2 stated that SOI-2 had purchased kilogram quantities of cocaine hydrochloride from STOREY since 2015. SOI-2 advised that SOI-2 would communicate with STOREY over a cellular device to arrange narcotic transactions and the delivery of controlled substances to Lynchburg, VA.

12. In September 2019, this applicant made contact with Source of Information #3 ("SOI-3") who stated that SOI-3 had a previous relationship of purchasing cocaine from STOREY. This applicant directed SOI-3 to conduct a recorded phone call with STOREY to purchase four ounces of cocaine hydrochloride. SOI-3 made contact with STOREY. STOREY instructed SOI-3 to travel to Charlotte, NC to purchase the cocaine. SOI-3 ultimately did not go through with the purchase.

13. In October 2019, the DEA Roanoke Resident Office (RRO) served an Administrative Subpoena on American Airlines for any reservation data regarding Jermel STOREY. A representative of American Airlines provided DEA RRO with the requested data. Based on that data, it was determined that STOREY provided an address of 6439 Quarterbridge Lane, Charlotte NC.

14. On December 3, 2019, a Grand Jury, of the United States Western District of Virginia, issued a Grand Jury Subpoena requesting Apple, Inc. to turn over records and information associated with JACESTOREY4@ICLOUD.COM. Based on the data received from Apple, Inc, this applicant determined that "Jermel Storey" of 6439 Quarterbridge Lane, Charlotte, NC was the name and listed address associated with that account. The cellular phone number 7047337054 was also attached to the Apple, Inc account. This account was created on June 22, 2016.

15. In February 2020, a Source of Information #4 ("SOI-4") was arrested in the Western District of Virginia for Distribution of cocaine and cocaine base. SOI-4 later advised law enforcement that STOREY had been SOI-4's source of supply for cocaine hydrochloride between 2016 through 2020. SOI-4 advised that STOREY had supplied the SOI-4 with approximately one hundred kilograms of cocaine during that timeframe. SOI-4 advised that he communicated with STOREY via cellular phone. SOI-4 advised that STOREY rotated to multiple "burner" phones, but that SOI-4 did not have STOREY's primary or personal number.

16. On June 4, 2020, United States Magistrate Judge Robert Ballou approved a search warrant (6:20MJ00016) authorizing the collection of data from a cellular phone seized from Co-Conspirator #1 ("CC-1"), a co-conspirator of STOREY. Analysis of that data recovered from that cellular phone revealed that CC-1 was in communication with numbers stored under the contact names of "JAH" and "SINSON". "JAH" and "SINSON" are known to be an alias for STOREY. Those text conversations referenced loss of money (investment) due to a law enforcement seizure of narcotics. CC-1 had previously been stopped by law enforcement and had a large amount of marijuana seized from him. Those texts messages also referenced the need to "reup" and other coded language that this affiant knows to be consistent narcotic trafficking.

17. Based on the overall investigation and previous search warrants executed in this case, there is probable cause to believe that STOREY has engaged in communications that constitute the evidence of drug trafficking and that those communications will be stored in data maintained by Apple, Inc. and associated with STOREY's iCloud account. STOREY's activity is believed to have been ongoing for multiple years, but beginning in at least June 2016 and continuing to the present.

INFORMATION REGARDING APPLE ID AND iCLOUD[1]

18. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

19. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages")

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

20. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

21. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

22. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including

the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

23. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

24. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC

address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

25. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

26. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the

files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

27. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

28. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

29. Based on the investigation, it is believed that STOREY is earning substantial profits from the drug distribution. Records obtained through the investigation show STOREY is using MoneyGram to send funds and banking at WoodForest National Bank and Wells Fargo National bank. Based on STOREY's banking activity, it is likely STOREY utilizes applications on his phone for banking and financial services that could lead to evidence of money laundering. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and

contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

30. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

31. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

32. Based on the forgoing, I request that the Court issue the proposed search warrant.

33. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

34. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/Daniel Bailey
Daniel Bailey, Task Force Officer
Drug Enforcement Administration

Received by reliable electronic means and sworn and attested to by telephone on this 21st day of July 2020.

Robert S. Ballou
ROBERT S. BALLOU
UNITED STATES MAGISTRATE JUDGE